

内部不正を見抜く： 小売業における隠 れたリスクと 検出戦略

組織的犯罪の影に潜む「動機」と
「機会」をコントロールする



Based on "How to Detect Internal Dishonesty"
by Cory Lowe, PhD & John Matas, CFE, CFCI (LPM, Feb 2026).
Translated/Summarized by JEAS (Japan Electronic Security Association).

NotebookLM

Forensic Editorial

暴力的な組織犯罪という「ノイズ」が、 静かなる内部不正の「シグナル」を隠している



- 小売業者は過去5年間、目に見える暴力やORCへの懸念を表明してきたが、内部不正が減少した証拠はない。
- サプライチェーンの複雑化（配送、販売チャンネルの拡大）により、不正の機会はむしろ増加している。

Insight: 内部不正は警察の介入なしに企業が自律的に解決できる領域であり、対策の効果果が最も出やすい。

NotebookLM

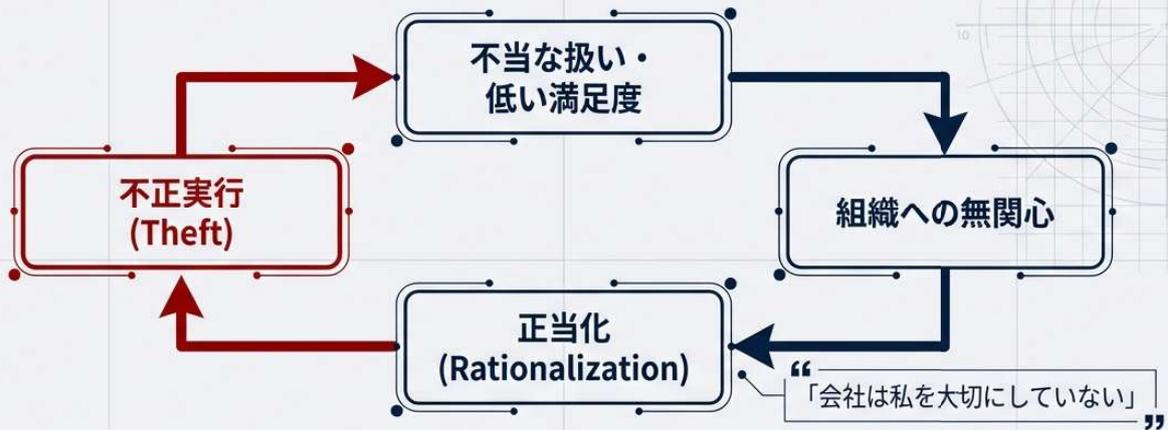
不正は「動機」と「機会」が交差する場所で発生する



- 従業員の個人的な経済ストレス（動機）を企業が完全に排除することは難しい。
- しかし、企業は「機会」と「監督」をコントロールすることができる。

❶ • **Key Takeaway:** 戦略の核心は「機会の削減」にある。

職場環境への不満が、不正を正当化する心理を生み出す



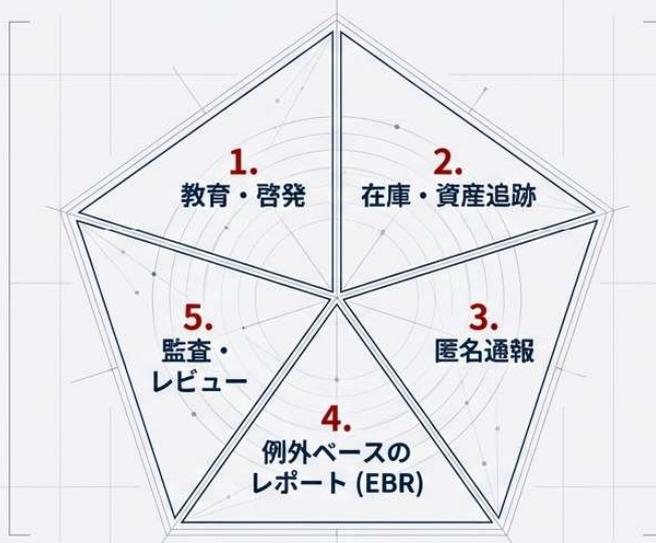
⚙️ **Risk Factors:** 経営陣への不満、経済的困難、不公平感、不明確な倫理規範。

💬 **The Rationalization:** 従業員は「雇用主は私を信頼も支援もしていない。なぜ私が会社の利益を守らなければならないのか？」と自問し、不正を正当化する。

🏢 **Cultural Impact:** 企業文化が手抜きや非倫理的な行動を黙認すると、不正が常態化する。

リスクを可視化し、抑止するための5つの防衛レイヤー

Forensic Editorial

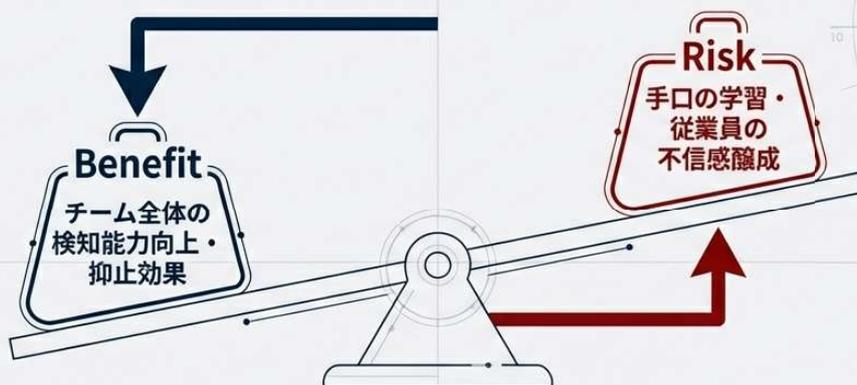


単一の解決策では不十分である。これら5つの手法を、リスクの高さに応じて階層的に組み合わせる「レイヤード・プログラム」が必要となる。

NotebookLM

Forensic Editorial

#1 教育と啓発：抑止力と不信感のバランス



⚙️ Strategy

従業員がLP（ロスプリベンション）プログラムの存在を知らなければ、抑止効果は限定的である。

⚠️ Warning

研修が攻撃的すぎると、「会社から疑われている」という敵対心を生み、逆効果になる可能性がある。

✅ Best Practice

離職率が高い環境でも、継続的な教育を維持する仕組みが必要。

NotebookLM

#2 在庫追跡：EASからRFIDへ—「何が」なくなったかを正確に知る



EASは「持ち出されたこと」しか分からないが、RFIDは「何が、いつ、どこから、誰によって」持ち出されたかを特定できる。

- ⚠ Internal Drift: 倉庫から商品が移動したが、売場にも補充されず、POSでも売れていない=内部不正の兆候。
- ⚙ Hybrid Approach: RFIDが未導入でも、高リスク商品の頻繁なサイクルカウントとビデオ検証の統合は不可欠。

#3 匿名通報：現場の「目」を活かすフィードバックループ



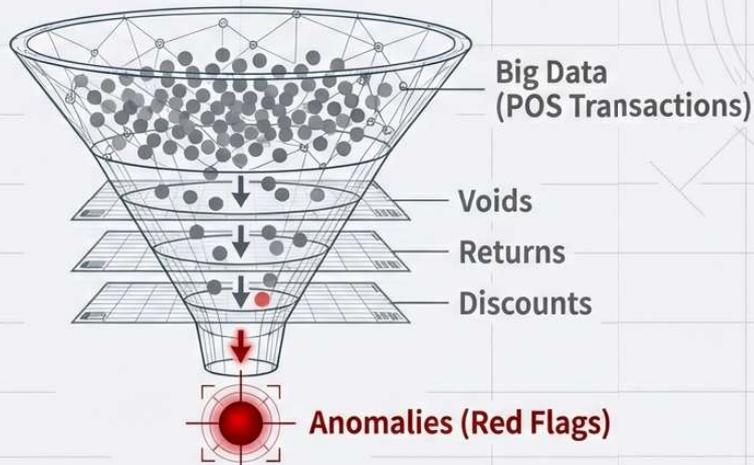
The Insight: 従業員は常に同僚と接しており、管理者よりも早く不正に気づく。最も費用対効果が高い手法。

Critical Success Factor: 「通報しても何も変わらない」と思われた瞬間、制度は死ぬ。結果をフィードバックし、行動が取られたことを示す必要がある。

Data Integration: 曖昧な通報でも、EBRや監査データと組み合わせることで調査の方向性を決定できる。

Forensic Editorial

#4 EBR (例外ベース管理) : 正常なデータフローから「異常」を抽出する



Mechanism: 取消、返品、値引、空打ちなど、標準から外れた「例外」操作が突出している従業員を特定する。

Advanced EBR: 従業員のシフトデータや店舗のトラフィック、さらにはゴミ捨て場の利用頻度（ビデオ分析）など、クロスチャネルでの異常検知が可能。

Requirement: データがデジタル化され、分析可能な状態でなければならない（手書き台帳は分析不可）。

Forensic Editorial

#5 監査とレビュー : デジタルの死角を物理的に検証する

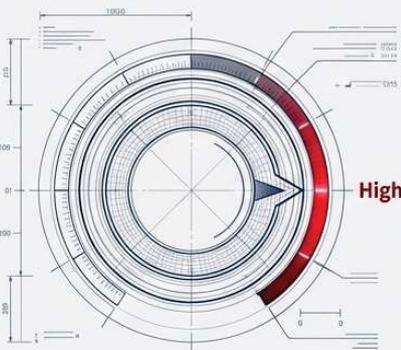
監査は単に犯人を見つけるだけでなく、「不正を可能にしているプロセスの欠陥」を明らかにする。

Focus: 全てを監査するのではなく、EBRや通報でリスクが示唆された領域にリソースを集中させる。

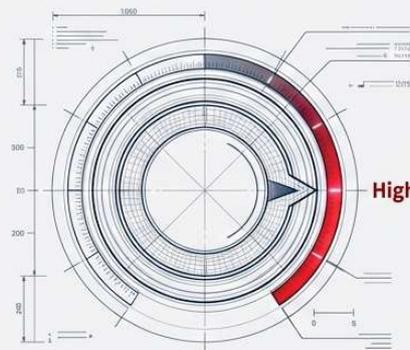


状況的犯罪予防 (LPRCモデル) の3つのレバー

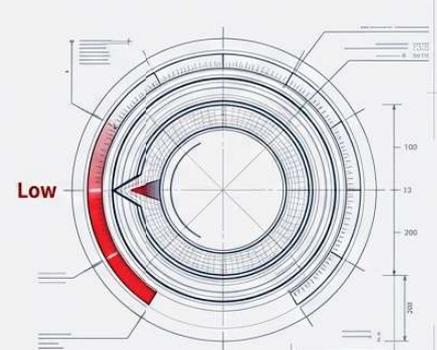
フロリダ大学ロスプリベンション研究評議会 (LPRC) に基づくアプローチ。
環境や状況を修正することで、従業員が「割に合わない」と感じる状況を作り出す。



労力を増やす
(Increase Effort)



リスクを高める
(Increase Risk)



利益を減らす
(Reduce Rewards)

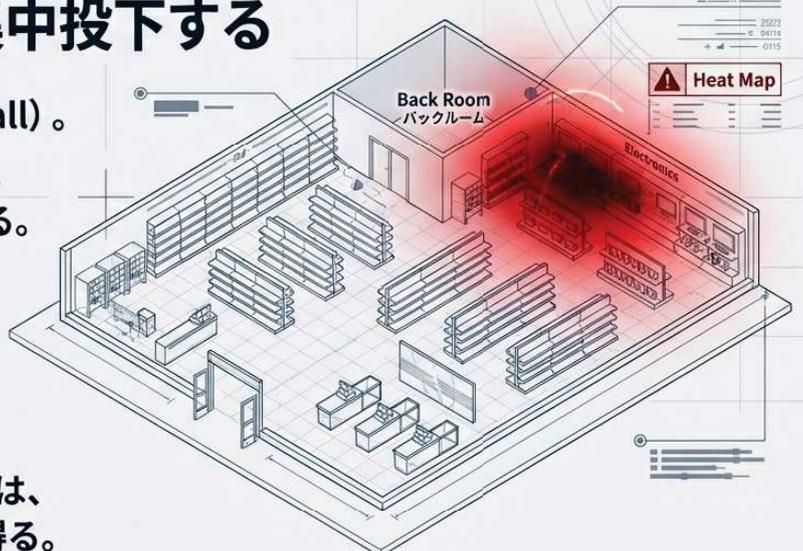
リスクベース・アプローチ：リソースを「高リスク領域」に集中投下する

Don't: 一律の対策 (One size fits all)。

Do: 以下の指標が高い店舗・部門にリソース (5つの手法) を集中させる。

- 離職率が高い
- 従業員満足度 (ES) が低い
- 在庫ロス率の異常

Insight: 感情データ (士気の低下) は、実際の不正発生の先行指標となり得る。



エグゼクティブ・サマリー：内部不正対策チェックリスト

- 文化の診断: 従業員の不満や不公平感を放置していないか？
- 教育のバランス: 抑止と信頼のバランスが取れた研修を行っているか？
- 可視化: RFIDやEBRを活用し、モノとデータの動きを追跡しているか？
- 通報制度: 通報者へのフィードバック（是正措置）は機能しているか？
- リスク集中: 離職率や士気データを基に、高リスク店舗を特定しているか？

内部不正は「発見」するものではなく、適切な戦略によって「管理」するものである。